CLAIMS

1. A method for enabling strong mutual authentication on a computer network comprising the steps of:

transmitting a first indicia to a first computer over a first communication channel;

generating by said first computer a first authentication number, a second authentication number, and a third authentication number;

transmitting by said first computer a first message to a second computer, wherein said first message comprises said first authentication number encrypted by said second authentication number;

transmitting by said first computer a second message to a verifier over a second communication channel, wherein said second message comprises said second authentication number encrypted and said third authentication number;

decrypting by said verifier said second message to obtain a first decrypted message, wherein said first decrypted message comprises said second authentication number;

transmitting by said verifier said second authentication number to said second computer

over a third communication channel;

decrypting by said second computer said first message transmitted by said first computer to recover said first authentication number;

transmitting by said second computer a third message to said first computer over said first communication channel, wherein said third message comprises said second authentication number encrypted by said first authentication number; and

validating said second computer by said first computer by decrypting said third message to obtain said second authentication number.

2. The method of claim 1, wherein said first authentication number is a session number.

3. The method of claim 1, wherein said first indicia is login information of a user for the said first computer.

4. The method of claim 1, wherein said second authentication number is a random number.

5. The method of claim 1, wherein said third authentication number is a random number.

6. The method of claim 1, wherein said first message further comprises said first authentication number encrypted with said second authentication number.

7. The method of claim 1, wherein said second message further comprises an encrypted portion.

8. The method of claim 7, wherein said encrypted portion further comprises said second authentication number encrypted in response to said first indicia.

9. The method of claim 8, wherein said encrypted portion further comprises said first indicia encrypted with a private key.

10. The method of claim 1, wherein said first decrypted message is decrypted by said verifier to validate said first computer to said verifier by recovering said third authentication number from said first decrypted message.

11. The method of claim 1, wherein said third message further comprises a third indicia.

12. The method of claim 11, wherein said third indicia and said second authentication number are encrypted with said first authentication number.

13. The method of claim 1, wherein said first communication channel is a confidential communication channel.

14. The method of claim 7, wherein said verifier has tamperproof memory and processing to ensure the validity of said second message or said encrypted portion of said second message.

15. The method of claim 1, wherein said third communication channel is an output device.

16. The method of claim 1, wherein transmitting said second message further comprises the steps of starting a clock by said first computer and measuring a timeout period by said clock

wherein said timeout period defines the period of time during which said third message must be received by said first computer.

17. The method for authenticating a third device to a first device comprising the steps of:

encrypting a first key with a second key by said first device encrypting said second key with a third key by said first device;

decrypting said encrypted second key in response to said third key by a second device; and

decrypting by said third device said encrypted first key using said second key obtained from said second device.

18. The method of claim 17 further comprising the step of encrypting said second key with said first key by said third device.

19. The method of claim 18 further comprising the step of decrypting said encrypted second key using said first key by said first device.

20. The method of claim 19 further comprising the step of comparing said second key decrypted using said first key with said second key used to encrypt said first key by said first device.

21. The method for authenticating a third device to a first device comprising the steps of:

transmitting by said first device a first message to said third device;

transmitting by said first device a second message to a second device;

transmitting by said second device a second key of said second message to said third device; and

obtaining by said third device a first key of said first message using said second key of said second encrypted key.

22. The method of claim 21, wherein said first message comprises said first key encrypted by said second key.

23. The method of claim 21, wherein said second message further comprises an encrypted portion.

24. The method of claim 23, wherein said encrypted portion further comprises said second key encrypted by a public key.

25. The method of claim 21 further comprising transmitting by said third device a third message to said first device.

26. The method of claim 25, wherein said third message comprises said second key encrypted by said first key.

27. The method of claim 25 further comprising obtaining by said first device said second key of said third message using said first key of said first message.

28. The method of claim 27 further comprising said first device comparing said second key of said third message with said second key of said first message.

29. The method of claim 21, wherein transmitting said second message further comprises the steps of starting a clock by said first device and measuring a timeout period by said clock wherein said timeout period defines the period of time during which said third message must be received by said first device.

30. A system for enabling strong mutual authenticating comprising:

a first transmitter;

a first receiver in communication with said first transmitter;

an output device in communication with said first receiver;

a second receiver in communication with said output device;

a second transmitter; and

a comparator in communication with said second transmitter and said first transmitter,

wherein said first transmitter transmits a first message to said second receiver over a first communication channel;

wherein said first transmitter transmits a second message to said first receiver over a second communication channel;

wherein said output device transmits a second key derived from said second message to said second receiver over a third communication channel;

wherein said second transmitter transmits a third message to said comparator over said first communication channel;

wherein said comparator compares said second key of said third message with said second key of said first message;

31. The system of claim 30, wherein said first receiver further comprises a smart card.

32. The system of claim 31, wherein said smart card comprises a tamperproof storage.

33. The system of claim 32, wherein said smart card further comprises the identification of the positive identity of a user.

34. The system of claim 30, wherein said first transmitter encrypts a first key with said second key to produce said first message.

35. The system of claim 30, wherein said first transmitter constructs an encrypted portion to produce said second message.

36. The system of claim 35, wherein said first transmitter encrypts said second key to produce said encrypted portion.

37. The system of claim 30, wherein said first receiver obtains said second key by decrypting said second message with a public key.

38. The system of claim 37, wherein said first receiver retrieves said public key from its computer memory.

39. The system of claim 30, wherein said second receiver decrypts said first message with said second key received from said output device to obtain said first key.

40. The system of claim 39, wherein said second receiver encrypts said second key received from said output device with said first key of said first message to produce said third message.

41. The system of claim 30, wherein said comparator decrypts said third message to obtain said second key.

42. The system of claim 30, wherein said first communication channel is a confidential channel.

43. The system of claim 30, wherein said second communication channel is a confidential channel.

44. The system of claim 30, wherein said third communication channel is a confidential channel.

45. The system of claim 30, wherein said second communication channel is a cellular communication channel.

46. The system of claim 30 further comprises a first input device in communication with said second receiver and said output device.

47. The system of claim 46, wherein said output device is in communication with said first input device over a confidential communication channel.

48. The system of claim 30, wherein said first transmitter comprises a clock used to measure the time period between transmitting said second message to said first receiver and receiving said third message from said second transmitter.